CLAIMS

1-6. (Cancelled)

7. (Currently Amended) A ~~restricted data format~~ method ~~for a network infrastructure copy protection system~~, comprising:

receiving a digital content file for transmission across a distributed computer network, wherein the distributed computer network comprises an intermediate node;

examining data comprising the content file to determine whether the content file includes a restricted data format, the examining performed by the intermediate node within the distributed computer network;

transmitting the content file to a computer system comprising one or more endpoints when data comprising the content file does not include the restricted data format, wherein the computer system is located external to the distributed computer network; and

blocking transmission of the content file when data comprising the content file does include the restricted data format to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the content file to the computer system ~~a receiver~~.

8-10. (Cancelled)

11. (Currently Amended) The method of Claim 7 wherein the distributed computer network comprises ~~is~~ the Internet.

12. (Currently Amended) The method of Claim 7 wherein the examining is performed by one or more ~~a plurality of~~ routers within the distributed computer network.

13. (Currently Amended) The method of Claim 7 wherein the examining is performed by one or more ~~a plurality of~~ cache engines within the distributed computer network.

14-16. (Cancelled)

17. (Currently Amended) A method comprising:

receiving a digital content file for transmission across a distributed computer network;

examining the digital content file to determine whether the digital content file comprises one or more signatures, wherein the one or more signatures identify one or more senders that requested transmission of the digital content file across the distributed computer network; and

logging the digital content file and the one or more signatures in a log, wherein the log of the one or more signatures is maintained in the distributed computer network to determine an identity of the one or more senders of the digital content file, and wherein the one or more senders reside external to the distributed computer network.

18-20. (Cancelled)

21. (Currently Amended) A network device comprising:

a bus;

computer readable memory units connected to the ~~said~~ bus;

one or more processors coupled to the ~~said~~ bus ~~said computer readable memory units~~ for executing a digital signature method for a network infrastructure copy protection system, comprising:

examining a digital content file to determine whether the digital content file includes a digital signature, wherein the examining is performed within the distributed computer network;

logging the digital content file and the digital signature to create a file transmission log, wherein the file transmission log is maintained within the distributed computer network;

transmitting the digital content file when the digital content file includes the digital signature; ~~and~~

blocking transmission of the digital content file when the digital content file does not include the digital signature to prevent unauthorized downloading of copyrighted material, wherein the blocking is effected prior to a transmission of the digital content file to a receiver; and

identifying a sender of the digital content file according to the digital signature included in the file transmission log after the digital content file has been transmitted, wherein both the

sender and the receiver of the digital content file are located external to the distributed computer network.

22. (Previously Presented) The device of Claim 21 wherein the file transmission log is configured to maintain a plurality of digital signatures associated with a single digital content file, where each of the plurality of digital signatures is logged for a separate transmission of the digital content file.

23. (Previously Presented) The device of Claim 21 wherein the digital signature applied to the content file within the distributed computer network is logged to maintain a record for the content file and the digital signature when the content file is transmitted across the distributed computer network.

24. (Currently Amended) The device of Claim 21 wherein the distributed computer network comprises ~~is~~ the Internet.

25. (Currently Amended) The device of Claim 21 wherein the examining is performed by one or more ~~a plurality of~~ routers within the distributed computer network.

26. (Currently Amended) The device of Claim 21 wherein the examining is performed by one or more ~~a plurality of~~ cache engines within the distributed computer network.

27. (Currently Amended) A method comprising:

receiving a digital content file for transmission across a distributed computer network;

examining the digital content file for inclusion of a first digital signature, wherein the digital content file is examined within the distributed computer network;

logging the digital content file and the first digital signature, wherein the log is maintained within the distributed computer network;

verifying an authenticity of the first digital signature, wherein the first digital signature is associated with a first user located external to the distributed computer network;

transmitting the digital content file including the first digital signature;

receiving the digital content file;

examining the digital content file for inclusion of a second digital signature;

logging the digital content file and the second digital signature;

verifying an authenticity of the second digital signature, wherein the second digital signature is associated with a second user located external to the distributed computer network; and

transmitting the digital content file including the second digital signature.

28-29. (Cancelled)

30. (Currently Amended) A system comprising:

means for receiving a file for transmission across a distributed computer network;

means for examining the file to determine whether the file includes one or more signatures, the examining performed within the distributed computer network;

means for transmitting the file across the [[a]] distributed computer network when the content file includes ~~does not include~~ the one or more signatures;

means for blocking transmission of the file when the file does not include the one or more signatures, wherein the blocking is effected prior to a transmission of the file to a receiver, and wherein the receiver is located external to the distributed computer network; and

means for maintaining a log of the file and the one or more corresponding signatures, wherein the log is maintained within the distributed computer network to identify one or more senders of the file after the file has been transmitted across the distributed computer network, and wherein the one or more senders are located external to the distributed computer network.

31. (Currently Amended) A system comprising:

means for receiving a digital content file for transmission across a distributed computer network;

means for using at least one router located within the distributed computer network, wherein the at least one router is configured to log one or more digital signatures related to the digital content file to maintain a record for the digital content file and the related digital signatures, the record including the related digital signatures;

means for examining data comprising the digital content file to identify the one or more digital signatures;

means for transmitting the digital content file outside of the distributed computer network when the data comprising the digital content file includes ~~does not include~~ the one or more digital signatures; and

means for blocking the transmission of the digital content file when the data comprising the digital content file does not include the one or more digital signatures; and

means for analyzing the record to identify one or more senders associated with the one or more digital signatures, wherein the record is configured to maintain a plurality of digital signatures for a digital content file that is transmitted by the one or more ~~a plurality of~~ senders, and wherein the one or more senders are located external to the distributed computer network.

32. (Currently Amended) The system ~~method~~ of Claim 31 further comprising:

means for identifying the one or more ~~a plurality of~~ senders that transmitted the digital content file across the distributed network, wherein each of the one or more ~~plurality of~~ senders is associated with at least one ~~or more~~ of the ~~plurality of~~ digital signatures.

33. (Previously Presented) The method of Claim 7 further comprising:

examining data associated with the digital content file to identify one or more digital signatures associated with one or more senders of the digital content file;

maintaining a log of each transmission of the digital content file and the associated one or more digital signature; and

identifying the one or more senders from the log after the transmission of the digital content file.

34. (Previously Presented) The method of Claim 17 wherein the log is capable of maintaining a plurality of signatures associated with a single digital content file.

35. (Currently Amended) The method of Claim 34 further comprising:

identifying the one or more ~~a plurality of~~ senders associated with the plurality of signatures, wherein one or more of the plurality of signatures is logged each time the digital content file is transmitted across the distributed computer network.

36. (Previously Presented) The method of Claim 27 wherein a log is maintained of the digital content file and both of the corresponding first and second digital signatures.

37. (Previously Presented) The method of Claim 36 further comprising:

identifying the first and second users from the first and second digital signatures maintained in the log.

38. (Previously Presented) The system of Claim 30 wherein the log is configured to maintain a plurality of digital signatures for a single file that is transmitted multiple times across the distributed network.

39. (New) The system of claim 31 wherein the record logging the digital content file and the related digital signatures is maintained within the distributed computer network.